512-CD-002-001

EOSDIS Core System Project

Release B Maintainability Demonstration Test Plans for the ECS Project

This document has not yet been approved by the Government for general use or distribution.

January 1998

Raytheon Systems Company
Upper Marlboro, Maryland

Release B Maintainability Demonstration Test Plans for the ECS Project

January 1998

Prepared Under Contract NAS5-60000
CDRL Item # 085

SUBMITTED BY

Deborah P. Dunn /s/ 1/22/98

Debbie Dunn, FOS CCB Chairman Date
EOSDIS Core System Project

Raytheon Systems Company
Upper Marlboro, Maryland

512-CD-002-001

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code 1, requires Government review and approval prior to acceptance and use, and is under ECS contractor configuration control. Once this document is approved, Contractor approved changes are handled in accordance with Class I and Class II change control requirements described in the EOS Configuration Management Plan, and changes to this document shall be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Drive
Upper Marlboro, Maryland 20774-5372

This page intentionally left blank.

Abstract

The Maintainability Demonstration (MD) Test Plans restate the requirements and objectives for conducting MD tests of ECS Commercial Off-the-Shelf (COTS) hardware (HW). The test plans attached are based upon accepted DID 511 MD failure scenarios for Release B, which meet the defined MD objectives, and correlate with planned Acceptance Test (AT) test procedures. The test plans describe testing requirements, methodology, step-by-step procedure, expected results, and success criteria. The test plans are accurate and complete as of this submission, but subject to further change and red lines as a result of dry run or formal testing.

Keywords: Maintainability; mean down time (MDT); failure; COTS; HW; Reliability, Maintainability, and Availability (RMA); repair; fault; diagnostics; spares; maintenance

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Original
iii through x	Original
1-1 through 1-2	Original
2-1 through 2-2	Original
3-1 through 3-4	Original
4-1 through 4-2	Original
A-1 through A-8	Original
B-1 through B-30	Original
AB-1 through AB-2	Original

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
512-CD-002-001	Original	January 1998	97-1768

This page intentionally left blank.

Contents

4. Maintainability Demonstration (MD) Process and Objectives

Tables

Appendix A. Failure Scenarios

Appendix B. FOS Test Plan

Abbreviations and Acronyms

1. Introduction

1.1 Identification

This document, Contract Data Requirements List (CDRL) item 085, the requirements of which are specified in Data Item Description (DID) 512/PA1, is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract NAS5-60000.

1.2 Scope

This document applies to COTS hardware (HW) selected, procured, integrated, and tested for an operational ECS Release. The Maintainability Demonstration (MD) Plan DID 511 will be revised in the event of custom HW, but ECS is not planning to develop any custom HW. The MD Plan also does not apply to the maintainability of ECS-developed or COTS software (SW). This submission provides a Flight Operations Segment (FOS) MD test plan that meets the defined FOS MD objectives, but is subject to further change and red lines as a result of dry run or formal testing. DID 512 will also be updated with the Science MD test plans when they are available. The ECS COTS HW has been designed to commercial maintainability standards and support practices. Therefore, these MD test plans do not verify unit level COTS Mean Time to Repair (MTTR) or commercial maintainability design.

This document reflects the February 7, 1996, Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS Technical Direction #11, dated December 6, 1994.

1.3 Purpose

The MD test plans restate the requirements and objectives for conducting MD tests of ECS COTS HW. The test plans attached are based upon accepted DID 511 MD failure scenarios for Release B, meet the defined MD objectives, and correlate with planned Acceptance Test (AT) test procedures. The test plans also describe testing requirements, methodology, step-by-step procedure, expected results, and success criteria; and are accurate and complete as of this submission, but subject to further change and red lines as a result of dry run or formal testing.

1.4 Status and Schedule

DID 511 for Release B was delivered and approved as one plan including both FOS and Science failure scenarios, and DID 512 will also be delivered as one document. Since schedule timing differences exist between FOS and Science, the FOS test plan is being delivered now and DID 512 will be updated with the Science test plans when they are available in 1998. The attached FOS Release B SYS-2030B test procedure is included in dual CDRL 322-CD-007-002/ 411-CD-007-002.

1.5 Organization

The contents of this document are as follows:

Section 1: Introduction - Introduces the Maintainability Demonstration Plan scope, purpose, schedule, and document organization

Section 2: Related Documentation - Describes the parent and applicable documents useful in understanding the details of subjects discussed in this document

Section 3: ECS Maintainability Environment - Discusses COTS HW maintainability characteristics, Release B operations and maintenance planning, and ECS system functional RMA requirements

Section 4: MD Process and Objectives - Describes the implementation process for the MD Plan and the 3 MD objectives and how they are achieved.

Appendix A: Failure Scenarios - Failure scenarios MD 1-8.

Appendix B: FOS MD Test Plan

Abbreviations and Acronyms

2. Related Documentation

2.1 Parent Documents

The parent documents are the documents from which this MD test plan's scope and content are derived.

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Fight Center, Functional and Performance Requirements Specification for the EOSDIS Core System (ECS)

2.2 Applicable Documents

The following documents are referenced within this MD test plan or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume:

322-CD-007-002/ 411-CD-007-002	Flight Operations Segment (FOS) Release B Integration and Acceptance Test Procedures for the ECS Project -- Merged Submission
511-CD-002-002	Release B Maintainability Demonstration Plan for the ECS Project
517-CD-001-004	Release B Failure Modes and Effects Analysis and Critical Items List for the ECS Project
613-CD-003-001	Release B COTS Maintenance Plan for the ECS Project

This page intentionally left blank.

3. ECS Maintainability Environment

3.1 COTS Hardware

The ECS HW for Release B and Release B FOS is COTS, with no custom HW or modified COTS planned or expected. The COTS HW has been designed and built to commercial maintainability standards and practices. This characterizes the COTS HW in the following ways:

a. Modular in design and fabrication

b. Designed to efficiently troubleshoot and maintain

c. Maintained by isolating failures to and replacing Line Replaceable Units (LRUs)

d. Typical Mean Time To Repair (MTTR) from 1/2 to 1 hour

e. Some level of vendor diagnostics to assist in trouble shooting

f. No preventive maintenance normally required

g. No special tools or test equipment normally required

Most COTS HW manufacturers offer warranty and extended warranty maintenance support for their products through their own service and support organizations. These manufacturers are, therefore, motivated to design in maintainability to minimize their own support time and material costs. Their maintenance technicians are generally well trained, certified, and have access to sophisticated diagnostics and back-up help desks.

These COTS maintainability factors support a MD planning approach that assumes the inherent commercial maintainability of ECS COTS HW and does not require evaluating the maintainability design or demonstrating the MTTR of any unit level COTS HW product.

3.2 ECS Maintenance and Operations

Once operations commence, COTS maintenance coverage to the Distributed Active Archive Centers (DAACs), System Monitoring and Coordination Center (SMC), and EOS Operations Center (EOC) will be consistent with the operations requirements of ECS-supported missions (e.g. AM-1, Landsat 7, etc.). Because of the higher costs of maintenance support during extended operations hours (i.e. nights, weekends, and holidays), maintenance coverage during these periods will be tailored to that required to sustain mission-critical operations and satisfy ECS A_O and MDT requirements. The minimum principal period of maintenance (PPM) at the DAACs, SMC, and ECS Development Facility (EDF) will be from 8AM to 5PM local time, Monday through Friday, excluding local holidays. The EOC provides 24-hour, 7-day-a-week maintenance coverage.

An on-site maintenance capability is provided by local maintenance coordinators (LMCs) to satisfy the operational availability and MDT requirements for some ECS functions (e.g. communications and science processing). Factors considered in the selection of COTS HW to be maintained by LMCs include criticality of the equipment and redundancy of components/systems; technical expertise needed to diagnose and replace failed LRUs; and the cost of training, spares, and support equipment.

LMCs may be trained and certified to perform maintenance on selected ECS equipment. When the LMC has been designated as the principal maintenance provider for COTS HW and SW, the LMC's responsibilities include fault diagnostics and identification to the LRU level, replacement of specified failed LRUs, or escalation of the problem to the responsible COTS contractor or the SMC for further assistance in diagnosing the cause of the problem.

When a COTS problem occurs, the LMC uses diagnostics tools, such as OpenView and built-in diagnostics, to identify and isolate the problem to the malfunctioning component, which may be SW or a failed LRU. If HW is identified as the source, the LMC or maintenance subcontractor corrects the problem by replacing the failed LRU, putting the unit back into operation, and testing the equipment and subsystem to verify the problem has been corrected.

Site engineering staffs and their LMC may be unable to resolve some of the more difficult maintenance problems. For this reason, backup support is available from a number of sources, including the SMC, Sustaining Engineering Organizations (SEO), maintenance subcontractors, and Original Equipment Manufacturers (OEMs). The LMC, following local procedures and ECS policy, determines if backup support is required based upon the nature of the problem. Network and SW-related problems may be referred to the SMC for assistance, while HW problems are normally referred to the local COTS HW maintenance subcontractor for resolution.

3.3 Operational Availability (A_O) and Mean Down Time (MDT)

The ECS A_O and MDT requirements differ between the FOS, Science Data Processing Segment (SDPS), and Communications and Systems Management Segment (CSMS) functions, depending on the criticality of the function involved. The specific A_O and MDT objectives for the segments and functions within segments are stated in Section 5 of GSFC 423-41-02, Revision A, dated June 2, 1994, and are shown in Table 3-1, "ECS Operational Requirements." It is emphasized that these requirements do not apply to individual/unit level COTS HW products, but rather to the entire system or subsystem function as indicated in the table.

Downtime has the greatest influence on achieving A_O in the mathematical relationship and also is emphasized through its own MDT requirements. These are downtime averages (mean) across all COTS HW failures in the function over a period of time. When averaging multiple failures, those with long downtime delays can be offset by short downtime switchover corrected failures in the computation of the MDT. The MDT requirement is not a discrete amount of time allowed for each individual unit level failure and should not be measured or demonstrated as such.

Table 3-1. ECS Operational Requirements

ECS Function	Functions	A_O Minimum	MDT Maximum
Flight Operations Segment (FOS)			
3800	Critical Real-Time Functions*	0.9998	1 min
3810	Non-Critical Real-Time Functions*	0.99925	5 mins
3820	Targets of Opportunity (TOO) *	0.992	1 hr
3700	ECS Functions not otherwise specified	0.96	4 hrs
3710	ECS shall have no single point of failure for functions associated with real-time operations of the spacecraft and instruments.		
Science Data Processing Segment (SDPS)			
3900	Science Data Receiving	0.999	2 hrs
3910	Switchover from Primary Science Data Receipt to Backup	NA	15 mins maximum not MDT
3920	Archiving & Distributing Data	0.98	2 hrs
3930	User Interfaces to Information Management System (IMS) Services at DAACs	0.993	2 hrs
3940	Information Searches on the ECS Directory	0.993	2 hrs
3950	Data Acquisition Request Submittals including TOOs*	0.993	2 hrs
3960	Metadata Ingest and Update	0.96	4 hrs
3970	Information Searches on Local Holdings	0.96	4 hrs
3980	Local Data Order Submission	0.96	4 hrs
3990	Data Order Submission Across DAACs	0.96	4 hrs
4000	IMS Data Base Management and Maintenance Interface	0.96	4 hrs
4010	Product Generation Computers	0.95	NA
4020	Product generation computers shall provide a “Fail soft” environment.		
Communications and System Monitoring Segment (CSMS)			
4030	SMC function of gathering and disseminating system management information for critical services	0.998	20 mins
4035	EOSDIS Science Network (ESN) shall have no single point of failure for functions associated with network databases and configuration data.		
4036	ESN A_O shall be consistent with the specified A_O of the ECS functions.		
3630	Maximum down time shall not exceed twice the required MDT in 99 percent of failure occurrences.		

A_O = Operational Availability
MDT= Mean Down Time
NA=Network Administrator

* = Required for Release B and subsequent releases only (all other functions required for Release 1 and subsequent releases)

This page intentionally left blank.

4. Maintainability Demonstration (MD) Process and Objectives

4.1 Process

The EOS Performance Assurance Requirements (PAR) for the ECS GSFC 420-05-03, in RMA section 5.6 presents the MD process and objectives. In accordance with this guidance, DID 511 presented proposed failure scenarios that have been approved to achieve the MD objectives. These scenarios are documented as test plans in DID 512 and will be conducted as part of the AT program. The test plans are being coordinated with existing AT and Verification test procedures with similar objectives. AT test procedures and MD test plans with the same objectives are coordinated into one testing activity serving both needs, rather than accomplishing redundant tests. This coordination is demonstrated by the use of FOS Test Case SYS-2030B in Attachment B, FOS Test Plan. This coordination of activities will be described appropriately in the MD Test Report DID 519.

4.2 MD Objectives

The PAR Section 5.6 and DID 511 establish three objectives for the MDs. These objectives are discussed below and related to the specific MD failure scenarios in Appendix A, Failure Scenarios.

4.2.1 Verify Capability to Meet A_O and MDT

The objective of the demonstrations as stated in the PAR is to verify the capability of the planned maintenance activities to meet the operational availability/MDTs stated in the ECS Functional and Performance Specification for identified system functions. The PAR section 5.6 identifies the system functions as the critical real-time system functions (primarily in the FOS).

As discussed in Section 3.3, the Functional and Performance specification RMA requirements are system function requirements applying across all the COTS HW implementing that function. An MD test, however, is normally accomplished on one individual unit level COTS product, and any resulting downtime measure for ECS would not represent all the COTS HW in the function for the given time period. Also, A_O is not directly measurable through an MD test; but, the principal component downtime is.

ECS critical real-time system functions are specified and exist only in the FOS. Since the MDT requirements for these are 1 minute or less, they are only achievable through HW redundancy in the design and SW switchover in the event of failure. This switchover is demonstrable through MD tests and will achieve this MD objective. Failure scenarios to demonstrate switchover are proposed for the FOS critical real-time functions during Release B and are included in Appendix A as scenarios MD - 6 and 8 for Release B. The applicable test plan is the FOS Test Case SYS-2030B (Failure Recovery and Status Monitoring) included as Attachment B.

In these scenarios, it is not intended to demonstrate the mean of MDT through a sample size and series of tests, but rather to demonstrate the capability to achieve the MDT during operations. This can be demonstrated in one MD test for each scenario by accomplishing failover or switchover within the required MDT time.

FOS Critical Command and Control Systems are systems that provide critical real-time functions to support the following: launch, early orbit checkout, disposal, orbit adjustment, anomaly investigation, recovery from safe mode, routine real-time commanding and associated monitoring for spacecraft, and instrument health and safety. This includes the execution and control of the ground script; the uplink of spacecraft loads, instrument loads, and real-time commands; command verification; ingest and monitoring of the real-time housekeeping telemetry and replay telemetry; and the capture and recording of real-time deviations to the planned ground script to ensure that the as-flown ground script is accurate.

For Release B, the FOS Critical Command and Control Systems that perform critical real-time functions consist of redundant groups of Real-Time Servers, Data Servers (for Events archiving function only), User Stations, RAID (Redundant Array of Independent Disks) storage devices, Time Systems, and network equipment (concentrators and hub/bridge assemblies).

4.2.2 Evaluate Fault Detection/Isolation Methods

The Management Subsystem (MSS) Fault Management Application Service will be implemented in Release B and demonstrated in each of the proposed failure scenarios as the primary fault-detection capability. Alerts and reports may initiate further fault/failure isolation and subsequent trouble shooting using COTS diagnostic tools as appropriate. All the proposed science failure scenarios MD 1-4 evaluate this fault detection objective.

4.2.3 Evaluate Ability to Achieve Line Replacement Unit (LRU) Replacements Onsite

The intent of this objective is to conduct a non-quantified evaluation of the on-site maintenance capability, consistent with the COTS Maintenance Plan. An analysis of the COTS maintenance processes to be implemented during Release B on-site and evaluation of the training, certification, and proficiency of assigned personnel will achieve this objective. Also, a review and analysis of the COTS HW failure activities in the EDF over the last 2 years will provide assessment of the vendor OEM and third-party maintenance processes in effect. It is recognized that the vendor-response times effective for the EDF are not as stringent as will be required for on-site operations. No MD failure scenario specific to these maintenance process evaluations is proposed.

Release B COTS will also be under vendor warranty during the AT period, and a COTS HW failure after detection, isolation, and confirmation of HW failure will be corrected onsite by the OEM warranty vendor. This unplanned, unrehearsed failure activity will also provide a demonstration and assessment of this maintenance approach. The fault-detection activities, operator response, local maintenance coordinator diagnosis and fault isolation process, OEM vendor contact and support, LRU identification and changeout, vendor spares positioning and availability, corrective action verification, and maintenance data collection can all be observed and analyzed as unplanned and unrehearsed actions. This unscheduled opportunity provides a demonstration of real failure OEM corrective-action processes.

Appendix A. Failure Scenarios

A.1 Evaluate Management Subsystem (MSS) Fault Management Application Service

Test No.: MD - 1 Release B

AT Test Case: **B080140.020 - Abnormal Non-Catastrophic Shutdown**

B080420.010 - On-Site Corrective Maintenance

Test Title: Evaluate Management Subsystem (MSS) Fault Management Application Service

Failure Scenario Description:

This scenario is designed to evaluate the capability, effectiveness, and usability of the Fault Management Service to detect, document, diagnose, isolate, provide impact status, and facilitate recovery from faults. The evaluation will be in the context of normal ECS on-site operations being interrupted by planned HW fault events or simulations with the focus on the effectiveness of this service in identifying and facilitating the accomplishment of corrective actions at the local site level. Local operator and local maintenance coordinator interactions with the service and its responsiveness and usability will be evaluated.

Input:

Standard ECS site operating environment; manual disconnection of the HW or network to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts; generated datasets.

Success Criteria:

Following HW failure, operators receive fault error messages detecting and isolating failure to the specific COTS HW. Appropriate diagnostics can be executed to further diagnose the specific HW fault and/or failed LRU. The Fault Management Service facilitates and assists the user, operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. The service facilitates and enhances the operator corrective action decision processes with accurate and useful operational status, recovery alternatives if available, and failure impacts to operations processes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.2 MSS Critical Services Failure Recovery

Test No.: MD - 2 Release B

AT Test Case : B080510.030 - RMA Assurance and Analysis

Test Title: MSS Critical Services Failure Recovery

Failure Scenario Description:

This scenario evaluates the failover design of the server providing the MSS Critical Services in meeting the MSS function RMA MDT requirement of 20 minutes or less. A fault event in the server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure, and local operator/administrator action will be taken to diagnose, isolate the failure, and initiate recovery corrective action. These diagnostic actions and switchover to the Failover Server and resumption of full Critical MSS Services should be completed within 20 minutes.

Input:

Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts, generated datasets.

Success Criteria:

Following HW failure, operators receive fault error messages detecting and isolating failure to the specific MSS Server. Appropriate diagnostics can be executed to further diagnose the specific HW fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. These diagnostic actions and switchover to the Failover MSS Server and resumption of full Critical MSS Services will be completed within 20 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.3 Primary Science Data Receipt Capability Failure Recovery

Test No.: MD - 3 Release B

AT Test Case : B080510.030 - RMA Assurance and Analysis

Test Title: Primary Science Data Receipt Capability Failure Recovery

Failure Scenario Description:

This scenario evaluates the failover design of the Ingest Server providing the primary science data receipt capability to meet the RMA function switchover time requirement of 15 minutes or less. A fault event in the Ingest Server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure and local operator/administrator action will be taken to diagnose and isolate the failure, and initiate recovery corrective action. These diagnostic actions and switchover time to the Failover server and resumption of full science data receipt services should be completed within 15 minutes.

Input:

Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts, generated datasets.

Success Criteria:

Following HW failure, operators receive fault error messages detecting and isolating failure to the specific Ingest Server. Appropriate diagnostics can be executed to further diagnose the specific HW fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. These diagnostic actions and switchover to the Failover Ingest Server and resumption of full Science Data Receipt Capability will be completed within 15 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.4 Network Failure Recovery

Test No.: MD - 4 Release B

AT Test Case: **B080620.020 - Network Fault Management**

Test Title: Network Failure Recovery

Failure Scenario Description:

This scenario evaluates the ability to detect, diagnose, analyze, and report network faults and errors at both the local site and SMC levels, and the local maintenance coordinator's responsiveness in taking appropriate corrective action. A network failure is simulated or a real component failure is introduced in a network HW device. The fault management capability will detect the failure and facilitate the isolation to the device and diagnosis of the problem. Appropriate reports and alerts will be generated. If the COTS network HW device is designed with hot swappable components, the failure will evaluate the local site's effectiveness in accomplishing the needed hot swap using available component LRUs. The hot swap can either be simulated or accomplished. The network will be maintained in normal operational status.

Input:

Standard ECS site operating environment; test procedure for the network HW device failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

Output:

Configuration status and fault event message displays/printouts, generated datasets.

Success Criteria:

Following network device failure, operators receive fault error messages detecting and isolating failure to the specific device. The network has remained operational with no data loss. Appropriate diagnostics can be executed to further diagnose the specific HW fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. If this test is a real hot swappable component failure, the changeout of the LRU is accomplished using on-site spares. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

A.5 FOS Network Fault Recovery

Test No.: MD - 5 Release B

AT Test Case: **SYS-2030B - Failure Recovery and Status Monitoring Test Procedure**

Test Title: FOS Network Fault Recovery

Failure Scenario Description:

This scenario is designed to verify the capability to recover from failures of network components supporting FOS operations, including the Operational LAN Fiber-optic Distributed Data Interface (FDDI), Ethernet and hub failures, and EOC router failure.

The scenario begins with the sign-on of several user stations and initialization of the EOC. A logical string supporting real-time, operational activities is created during EOC initialization. Configuration and event pages are displayed and used to verify the EOC configuration following logical string creation and reconfiguration activity performed by the user with ground configuration authority. Each type of failure listed above is performed sequentially, with test steps included to ensure the recovery from each failure.

During recovery operations, alphanumeric display pages showing the FOS configuration components and status are viewed and printed at specified times (i.e. before, during, and after failure recovery) to verify the accurate representation of configuration information throughout the recovery period.

Input:

Startup scripts for initializing the EOC, manual disassembling/disabling/disconnecting connected network components to simulate network/hub failures or to introduce real component failures.

Output:

Configuration status display pages/printouts and event displays/printouts at EOC/Instrument Support Terminal (IST) user stations.

Success Criteria:

Following FDDI and FDDI hub failures, FDDI ring wraps autonomously with no data loss and FOS SW applications continue as normal. During Ethernet failure, the EOC user stations on the Ethernet link lose connection to supported logical strings; the affected user station(s) successfully re-establishes former string connection on another EOC user station. Following EOC Router failure and recovery, no FOS reconfiguration is required; IST user stations, following ECS Command Language (ECL) directives to reconnect to established logical strings, are successful in connecting. Upon any network failure, connected EOC/IST user stations receive error messages concerning the failure and messages following network recovery. Configuration display pages accurately portray the FOS configuration before, during, and after network failures.

A.6 FOS Real-Time Server Failure Recovery

Test No.: MD - 6 Release B

AT Test Case: **SYS-2030B - Failure Recovery and Status Monitoring Test Procedure**

Test Title: FOS Real-Time Server Failure Recovery

Failure Scenario Description:

This scenario is designed to verify the capability to recover from a real-time server failure during real-time operations within a down time of 1 minute or less.

The scenario begins with the sign-on of several user stations and initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and receipt of real-time telemetry. The real-time server is disconnected/powered down to simulate a failure or a prepared component failure is introduced. Upon detecting telemetry data dropout and other event messages at connected EOC and IST user stations, the ground controller enters directives to transfer control to the backup, and specifies the real-time server that is to receive control and if checkpoint information (telemetry and command path information) is to be applied. As the backup logical string is converted to active, the ground controller requests command authority, resumes the ground script, and begins processing real-time telemetry.

Input:

Startup scripts for initializing the EOC; manual disassembling/disabling/disconnecting the real-time server to simulate server failure, or introduction of real component failure.

Output:

Configuration status and event message displays/printouts.

Success Criteria:

Following server failure, EOC/ISTs receive event messages stating real-time data dropout, pause of the ground schedule, and server failure events. Request of ground configuration authority is granted following failure of the server. Directives to transfer control to the backup real-time server and transfer checkpoint information are successful **and occur within 1 minute of the request.** Previously running ground script resumes upon ECL directives. EOC/IST users connected to the failed real-time server are re-established to previous logical strings upon re-issue of connection directives. Configuration display pages accurately portray the FOS configuration before, during, and after the real-time server failure.

A.7 FOS Data Server Failure and Recovery

Test No.: MD - 7 Release B

AT Test Case: **SYS-2030B - Failure Recovery and Status Monitoring Test Procedure**

Test Title: FOS Data Server Failure Recovery

Failure Scenario Description:

This scenario is designed to verify the capability to recover from a data server failure during real-time operations.

The scenario begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings. Several analysis requests for datasets are generated and submitted. During execution of the datasets, the data server is disconnected/powered down to simulate a failure or a prepared component failure is introduced. Upon detecting event messages stating communications failure with the data server, appropriate corrective actions are taken. Configuration display pages are printed before, during, and after failure recovery to ensure accurate portrayal of the FOS equipment configuration.

Input:

Startup scripts for initializing the EOC; manual disconnection of the data server to simulate a failure, or introduction of real component failure.

Output:

Configuration status and event message displays/printouts, generated datasets.

Success Criteria:

Following server failure, EOC/ISTs receive error messages stating communications failure of the data server. Initialization and startup of the non-active data server completes within 5 minutes. Configuration display pages accurately portray the FOS configuration before, during, and after the data server failure.

A.8 FOS User Station Failure Recovery

Test No.: MD - 8 Release B

AT Test Case: **SYS-2030B - Failure Recovery and Status Monitoring Test Procedure**

Test Title: FOS User Station Failure Recovery

Failure Scenario Description:

This scenario is designed to verify the capability to recover from a user station failure during real-time operations within a down time of 1 minute or less.

The scenario begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and receipt of real-time telemetry. The EOC user station currently operating as the ground controller/command issuer is disconnected/powered down to simulate a failure or a real prepared component failure is introduced. Upon detecting the failure, the ground controller transfers to another EOC user station, requests command authority, applies checkpoint information to the ground script, and resumes the script. Steps are also provided to ensure failure recovery from an IST user station failure.

Input:

Startup scripts for initializing the EOC, manually disconnecting the user station to simulate a failure or introduction of component failure.

Output:

Configuration status and event message displays/printouts.

Success Criteria:

Request of ground configuration authority, transfer of checkpoint files to the ground script, and resumption of the ground script is successful **within a down time of 1 minute or less**, following the issuance of the directives from another EOC user station. Configuration display pages accurately portray the FOS equipment configuration before, during, and after the user station failure. IST users experiencing failure conditions may sign on to another IST user station and perform functions mirroring their previous activity on the failed user station.

Appendix B. FOS Test Plan

Table B-1. Failure Recovery and Status Monitoring Test Procedure

Test Case No: SYS-2030B
Test Configuration: See Appendix G
Test Support: Powered-up FOS servers; Operational LAN and Support LAN; Primary EOC Router and Secondary EOC Router; one EOC user station that can perform Ground Control and Command activities; one EOC user station that can perform command activities; FOS Server startup scripts; PackGen telemetry driver; ground script with 'WAIT' directive; logical string and telemetry display pages.
Test Case Description: This test is designed to verify that the EOC has no single point of failure for functions associated with real-time operations, can quickly and properly recover from unscheduled software and hardware failures (including those associated with user stations, Real-Time Server, Data Server, File Server, and Network [ECS Router and LAN]), and provides status monitoring information on FOS resources. The FOS Servers, and EOC user stations are initialized, including connection to default String 100. EOC user station failures are induced, resulting in event messages, re-initialization, and switching command authority. Unsuccessful attempts are made to create a backup server for String 100 because either the user does not have Ground Control Authority or the active server is specified as the backup. After taking Ground Control and specifying the proper server, a backup server is successfully created for String 100. Server identification and other system parameters are inspected on a pre-built display page for the proper values. The flow of telemetry is initiated and monitored via pre-built display pages. A software failure of several key processes is induced on the Real-Time Server, resulting in Ground Script suspension and event messages. An ECL directive is used to initiate a failover from the active to the backup Real-Time Server. Event messages and display pages are inspected for messages on server status and updated ground system information, respectively. The Ground Script is resumed on the new, active Real-Time Server, and the Event Display is checked for associated messages. UNIX commands and Netscape are used to check access to data (files) and the data base.

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

The user specifies the former active Real-Time Server as the backup server. A hardware failure is induced on the current active Real-Time server, and an event message is generated. The same failover and post-failover check-out steps are executed as previously (i.e., resume executing the Ground Script, inspect display pages, and access files and the data base). Next, a major software failure is induced on the Data Server, but since there is no automated failover processing, the inactive Data Server is initialized using standard Data Server startup procedures. The same post-failure check-out steps are executed as before. A hardware failure is induced on the Data Server, followed by initialization of the inactive Data Server and post-failure check-out as before. Then a hardware failure is induced on the File Server; but, since there is permanent redundancy, the failover is automatic. The same post-failure check-out steps are executed as before. Next, the Primary EOC Router is powered off, and a script is executed to switch all applicable hardware to the Secondary EOC Router. The same post-failure check-out steps are executed as previously. Finally a failure is induced on the Operational LAN by powering down the applicable FDDI concentrators and Ethernet switches. A script is executed to switch all applicable hardware to the Support LAN. The same post-failure check-out steps are executed as before.
Success Criteria: This test is successful when the EOC has no single point of failure for functions associated with real-time operations; properly recovers from unscheduled software and hardware failures within the required time period, including one minute for real-time resources; and provides users with notifications and status monitoring information on EOC resources.

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

Step Id	Action	Expected Result/Output	Pass /Fail
1.	**Initialization follows.**	Only information, no result or output, is expected.	
2.	**EOC User Station 1**: Log in to an EOC user station that can perform Ground Control and Command activities, using the UNIX login procedure, by entering a valid User Name and Password: Username: **<user name>** Password: ************	The login is accepted and two cmdtool windows come up.	
3.	**EOC User Station 2**: Log in to an EOC user station that can perform Command activities, using the UNIX login procedure, by entering a User Name and Password that has command authority: Username: **<user name>** Password: ************	The login is accepted and two cmdtool windows come up.	
4.	**EOC User Station 1**: Execute the applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the Data Server. *(Wait for completion of Data Server startup.)*	The Data Server Startup initialization is complete.	
5.	**EOC User Stations 1 & 2**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) test procedure to bring up the EOC user stations. *(Wait for completion of user station startup.)*	The user station startup is complete when the Control Windows come up.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

6.	**EOC User Station 1**: Invoke the Global Event Display. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' menu, select 'Event_Display-Global.'	The 'Tools' menu comes up, then closes. The 'Event Display' comes up.	
7.	**EOC User Station 1**: Execute the applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the **active** Real-Time Server. Execute the applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the **non-active** Real-Time Server. *(These startup scripts can be executed simultaneously. However, wait for the completion of both Real-Time Server startups before going to the next step.)*	**Active** Real-Time Server Startup is complete when the following message appears in the Event Display: 'String 100 was created.' Non-active Real-Time Server Startup is complete when the following message appears in the Event Display: 'Successfully performed nameserver register on RMS PtToPt Endpoint'	
8.	**EOC User Station 1**: Connect to the default real-time operational string by entering the following in the ECL directive line of the Control Window: ECL> **STRING CONNECT STRING=100 CONFIG=MIRROR** *(Wait for string connection to complete.)*	After several minutes, the message 'Successfully connected to string 100' appears on the Event Display.	
9.	**The EOC User Station 2 Failure and Status Monitoring test follows.**	Only information, no result or output, is expected.	
10.	**EOC User Station 2**: Simulate a hardware failure by pulling the EOC User Station 2 plug connected to the LAN.	Within 3 minutes, an event message appears indicating EOC User Station 2 failure. The following message appears in the cmdtool (console) window: 'le0: No carrier - cable disconnected or hub link test disabled?'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

11.	**EOC User Station 2**: Re-insert the plug and terminate all FOS processes on EOC User Station 2 by entering the following in a cmdtool window: %: **MyKill** *(Wait until all processes terminate.)* Enter the following in a cmdtool window: %: **rm.sh**	The following message appears in the cmdtool (console) window: 'le0: NFS server opsraid OK.' All processes and endpoints are terminated.	
12.	**EOC User Station 2**: Execute the applicable steps of the 'FOS Server and User Station Startup' (SYS-2000B) test procedure to bring up EOC User Station 2. *(Wait for completion of user station startup.)*	User station startup is complete when the Control Window appears on EOC User Station 2. Within 3 minutes of user station startup completion, an event message appears indicating that EOC User Station 2 has come back up.	
13.	**EOC User Station 2**: Invoke the Global Event Display. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' menu, select 'Event_Display-Global.'	The 'Tools' menu comes up, then closes. The 'Event Display' comes up.	
14.	**EOC User Station 2**: Connect to the default real-time operational string by entering the following in the ECL directive line of the Control Window: ECL> **STRING CONNECT STRING=100 CONFIG=MIRROR** *(Wait for the string connection to complete before going to the next step.)*	After several minutes, the message 'Successfully connected to string 100' appears on the Event Display.	
15.	**EOC User Station 1 Failure During Commanding test follows.**	Only information, no result or output, is expected.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

16.	**EOC User Station 1 & 2**: Bring up the Failover-Monitoring display page. In the 'Control Window,' click on the 'TlmWins' button. In the 'Tlm Wins' menu, select 'Failover-Monitoring.	The Failover Monitoring page appears.	
17.	**EOC User Station 1**: Take Ground Control for String 100 by entering the following in the ECL directive line of the Control Window: ECL>**TAKE GROUNDCONTROL STRING=100**	The following event message is displayed: 'Ground Control authority has changed from <EcDNull or user> to <User #1> for String 100.' The current user is shown as the user with command authority (SYS_GRND_CNTRL_ID) on the Failover-Monitoring display page.	
18.	**EOC User Station 1**: Take command of String 100 by entering the following in the ECL directive line of the Control Window: ECL>**TAKE COMMAND STRING=100**	The following event message is displayed: 'Command authority has changed from <EcDNull or user> to <User #1> for String 100.' The current user is shown as the user with command authority (SYS_CMD_AUTHOR_ID) on the Failover-Monitoring display page.	
19.	**EOC User Station 2**: Print the Failover-Monitoring page just updated by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 1' column.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

20.	**EOC User Station 1**: Remotely log in to the Real-Time Server by entering the following in a new cmdtool window. %: **rlogin <RealTimeServer>** At the Real-Time Server prompt, enter the following: %: **cd/fosb/test/am1/scripts/setup** (**test** is alias) %: **setenv SCRIPT RealTimeServer** %: **source FosEnvVars** %: **cd/fosb/test/am1/bin/sun_sparc_5-5** (**bin** is alias) %: **sc AM1 100 Ops**	The remote login to the Real-Time Server is successful. The following message appears repeatedly in the Real-Time Server cmdtool window: 'sc Waiting for messages'	
21.	**EOC User Station 1**: Invoke the Command Control window. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' window, select 'Command_Control.'	The 'Tools' menu comes up, then closes. A dialog box appears allowing the user to enter String Id=100 and Spacecraft ID=AM1. The Command Control window is displayed.	
22.	**EOC User Station 1**: Initiate the tcpdump tool to capture **real-time**, **operational** commands. In a new cmdtool window, enter the following: %: **tcpdump -v port 20058**	The following message appears on User Station 1 in the cmdtool window: 'listening on le0'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

23.	**EOC User Station 1**: In the 'Config' pull-down menu of the 'Command Control Window,' set the following: Cmd Verification (CV): Off Tlm Verification (TV): Off In the 'Command Control Window,' enter the following in the CMD field: **FOP INIT CHECK** Then, click on the 'Resume' button. Click on the 'Send' button. Click on the 'Suspend' button.	**EOC User Station 1**: In the 'Command Control Window,' the following occurs: The 'CV' and 'TV' indicators are both 'Off.' The 'DIRECTIVE' column contains 'FOP INIT CHECK.' After the 'Resume' button is clicked, the Send/Cancel options are activated. After the 'Send' button is clicked, the STATUS column includes 'Processed -2 | Sent to subsys.' The following event messages appear: 'StringMgr process successfully configured'; 'Protocol Info: FOP INIT with CLCW check successful.'	
24.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages are generated for those Ground Script commands executed prior to the WAIT command, indicating successful execution.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

25.	**EOC User Station 1**: Simulate a hardware failure by pulling the EOC User Station 1 plug connected to the LAN (Ethernet Switch).	The remaining Ground Script commands cannot be executed. Within 1 minute, an event message appears indicating EOC User Station 1 failure: 'String 100 Ground Control user station, host name <user station 1>, unavailable' 'String 100 CommandAuthority user station, host name <user station 1>, unavailable' The following message appears in the cmdtool (console) window: 'le0: No carrier - cable disconnected or hub link test disabled?'	
26.	**EOC User Station 2**: Take Ground Control for String 100 by entering the following in the ECL directive line of the Control Window: ECL>**TAKE GROUNDCONTROL STRING=100**	The following event message is displayed: 'Ground Control authority has changed from <User #1> to <User #2> for String 100.' The current user is shown as the user with command authority (SYS_GRND_CNTRL_ID) on the Failover-Monitoring display page.	
27.	**EOC User Station 2**: Take command authority away from EOC User Station 1 by entering the following in the ECL directive line of the Control Window: ECL>**TAKE COMMAND STRING=100**	The following event message is displayed: 'Command authority has changed from <User #1> to <User #2> for String 100.' The current user is shown as the user with command authority (SYS_CMD_AUTHOR_ID) on the Failover-Monitoring display page.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

28.	**EOC User Station 2**: Print the Failover-Monitoring page just updated by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 2' column.	
29.	**EOC User Station 2**: Invoke the Command Control window. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' window, select 'Command_Control.	The 'Tools' menu comes up, then closes. A dialog box appears enabling the user to enter String Id=100 and Spacecraft. The Command Control window is displayed.	
30.	**EOC User Station 2**: Resume executing the remainder of the Ground Script.	Event messages are generated for the remaining Ground Script commands following the WAIT command, indicating successful execution. Note: The portion of the Ground Script executed prior to the failure should *not* be re-executed, commands not executed prior to the failure should *not* be skipped, and it should *not* be necessary to restart the Ground Script from the beginning.	
31.	**EOC User Station 1**: Re-insert the plug and terminate all processes on EOC User Station 1 by entering the following in the ECL directive line of the Control Window: %: **MyKill** *(Wait until all processes terminate.)* Enter the following in a cmdtool window: %: **rm.sh**	The cmdtool (console) window contains the message: 'NFS server supraid OK.' All processes and endpoints on EOC User Station 1 are terminated.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

32.	**EOC User Station 1**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) test procedure to bring up the EOC user station for FOS applications. *(Wait for the completion of the user station startup.)*	The user station startup is complete when the Control Window appears on the EOC user station. Within 3 minutes of user station startup completion, an event message appears indicating that EOC User Station 1 has come back up.	
33.	**EOC User Station 1**: Invoke the Global Event Display. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' menu, select 'Event_Display-Global.'	The 'Tools' menu comes up, then closes. The 'Event Display' comes up.	
34.	**EOC User Station 1**: Connect to the default real-time operational string by entering the following in the ECL directive line of the Control Window: ECL> **STRING CONNECT STRING=100 CONFIG=MIRROR** *(Wait for the string connection to complete before going to the next step.)*	After several minutes, the message 'Successfully connected to string 100' appears on the Event Display.	
35.	**EOC User Station 1**: Bring up the Failover-Monitoring display page. In the 'Control Window,' click on the 'TlmWins' button. In the 'Tlm Wins' menu, select 'Failover-Monitoring.	The Failover Monitoring page appears.	
36.	**EOC User Station 1**: Take command authority away from EOC User Station 2 by entering the following in the ECL directive line of the Control Window: ECL>**TAKE COMMAND STRING=100**	The following event message is displayed: 'Command authority has changed from <User #2> to <User #1> for String 100.' The current user is shown as the user with command authority (SYS_CMD_AUTHOR_ID) on the Failover-Monitoring display page.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

37.	**EOC User Station 1**: Invoke the Command Control window. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' window, select 'Command_Control.'	The 'Tools' menu comes up, then closes. A dialog box appears enabling the user to enter String Id=100 and Spacecraft ID=AM1. The Command Control window is displayed.	
38.	**The preparation for Real-Time Server Failover follows.**	Only information, no result or output, is expected.	
39.	**EOC User Station 1**: Print the Failover-Monitoring page just updated by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 3' column.	
40.	**EOC User Station 1**: Try to create a backup logical string on the **non-active** Real-Time Server connected to the Operational LAN by entering the following in the ECL directive line of the Control Window: ECL> **STRING CREATE BACKUP SERVER=2 STRING=100**	The backup string is **not** created (since the user does not have Ground Control authority). The following event message appears: 'User is not the Ground Controller for string 100. User must have Ground Control Authority before requesting this service.'	
41.	**EOC User Station 1**: Take Ground Control by entering the following in the ECL directive line of the Control Window: ECL> **TAKE GROUNDCONTROL STRING=100**	The Ground Control privilege is granted, and the following message appears on the Event Display: 'Ground Control Authority has been changed from EcDNull to <user>.' The current user is shown as the Ground Controller (SYS_GRND_CNTRL_ID) on the Failover-Monitoring display page.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

42.	**EOC User Station 1**: Try to create a backup logical string on the **active** Real-Time Server by entering the following in the ECL directive line of the Control Window: ECL> **STRING CREATE BACKUP SERVER=1 STRING=100**	The backup string is **not** created (since the active server cannot simultaneously be the backup server), and the following message appears on the Event Display: 'Unable to create Backup String on RTS xxx because active string processing exists on this RTS.'	
43.	**The Real-Time Server Software Failover test follows.**	Only information, no result or output, is expected.	
44.	**EOC User Station 1**: Create a backup logical string on the **non-active** Real-Time Server by entering the following in the ECL directive line of the Control Window: ECL> **STRING CREATE BACKUP SERVER=2 STRING=100** *(Wait for the completion of the backup directive before going to the next step.)*	The backup string is created, and the following message appears on the Event Display: 'Successfully created backup processing for string 100.'	
45.	**EOC User Station 1**: Print the Failover-Monitoring page by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 4' column.	
46.	**EOC User Station 1**: Display the number of endpoints for the **active Real-Time Server** by entering the following in a cmdtool window: %: **show.sh** (Note the number of endpoints.)	There are 33 endpoints on the active Real-Time Server: '(33 rows affected)'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

47.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages are generated for those Ground Script commands executed prior to the WAIT command, indicating successful execution.	
48.	**EOC User Station 1**: Bring up the Health & Safety telemetry decom display page, which displays telemetry packet information. In the 'Control Window,' click on the 'TlmWins' button. In the 'Tlm Wins' menu, select 'TLM-2000B.'	The 'Telemetry Window Selection' menu comes up, then closes. The 'TLM-2000B' Health & Safety telemetry decom display page comes up.	
49.	**EOC User Station 2**: Invoke the telemetry driver for the multicast of telemetry packets. In a new cmdtool window, enter the following: %: **cd/fosb/test/am1/scripts/setup** (**test** is alias) %: **setenv SCRIPT UserStation** %: **source FosEnvVars** %: **cd/fosb/test/am1/bin/sun_sparc_5-5** (**bin** is alias) %: **FtPgPackGen**	The following message appears in the window where the FtPgPackGen tool is running: 'Packet Generator is ready to receive directives.'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

50.	**EOC User Station 2**: Start the multicast of **real-time/operational/ I-channel housekeeping** telemetry packets for processing. Enter the following ECL directives: ECL> **PG CONFIG HOST=225.2.7.00 PORT=20002 APID=2** ECL> **PG STARTDATA APID=2 COUNT=-1** (Note: The IP address and port number is in the file '/fosb/test/am1/config/FoSwConfigData. cnfg.')	Telemetry values are updated on the 'TLM-2000B' Health & Safety Telemetry display page.	
51.	**EOC User Station 1**: Simulate a software failure by gracefully terminating the Ground Script Controller process on the active Real Time Server. Enter the following in a cmdtool window: %: **ps -ea** %: **kill -9 <Ground Script Controller process id>**	Within 60 seconds, an event message indicates that the Ground Script Controller process has been terminated: 'Active strand for string 100 failed due to failure of <process name> process. Suggest failover.' The Telemetry Decom page continues updating.	
52.	**EOC User Station 1**: Initiate the failover from the active Real-Time Server to the backup Real-Time Server by entering the following in the ECL directive line of the Control Window: ECL> **STRING FAILOVER STRING=100** *(Wait 60 seconds before executing the next step.)*	Within 60 seconds, the following occur: The Real-Time Server 1 is **temporarily** the **inactive** server until failover is complete. Event messages appear indicating that Real-Time Server 2 is coming up as the **active server**. Note: If the failover is unsuccessful (i.e., the backup and inactive servers are not both zero), an event message will appear notifying the user to delete String 100. The user would do this and then create String 100.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

53.	**EOC User Station 1**: Close the existing Failover Monitoring display page, and bring up a new Failover-Monitoring display page. In the 'Control Window,' click on the 'TlmWins' button. In the 'Tlm Wins' menu, select 'Failover-Monitoring.	The existing Failover Monitoring page closes, and the new Failover Monitoring display page appears.	
54.	**EOC User Station 1**: Print the Failover-Monitoring page by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 5' column.	
55.	**EOC User Station 1**: Display the number of endpoints for the **active Real-Time Server** by entering the following in a cmdtool window. %: **show.sh** Note the number of endpoints.	There are 33 endpoints on the active Real-Time Server: '(33 rows affected)'	
56.	**Post-Failure Check-out Subprocedure start** **EOC User Station 1**: Bring up a new Command Control window. In the 'Control Window,' click on the 'Tools' button. In the 'Tools' window, select 'Command_Control.'	The 'Tools' menu comes up, then closes. A dialog box appears enabling the user to enter String Id=100 and Spacecraft ID=AM1. The Command Control window is displayed.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

57.	**EOC User Station 1**: Resume executing the remainder of the Ground Script.	Event messages are generated for the remaining Ground Script commands following the WAIT command, indicating successful execution. Note: The portion of the Ground Script executed prior to the failure should *not* be re-executed, commands not executed prior to the failure should *not* be skipped, and it should *not* be necessary to restart the Ground Script from the beginning.	
58.	**EOC User Station 1**: Check access to FOS data by displaying the contents of a telemetry archive file. Enter the following in a cmdtool window. %: **ls -l/fosb/test/am1/tlmarchive**	A list of archive files is displayed.	
59.	**EOC User Station 1**: Check access to the FOS database by displaying information on system-level parameters via Netscape. Mnemonic: **SYS** Click on 'Submit' **Post-Failure Check-out Subprocedure end**	Information on system-level parameter mnemonics is displayed.	
60.	**EOC User Station 1**: Terminate all processes for all strings on **Real-Time Server 1** (the server on which processes were terminated) by entering the following in a cmdtool window associated with the Real-Time Server: %: **MyKill** *(Wait until the UNIX prompt is received.)* %: **rm.sh**	The number of endpoints for Real-Time Server 1 is zero.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

61.	**EOC User Station 1**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the **non-active** Real-Time Server (Server 1). *(Wait for the completion of the Real-Time Server startup before going to the next step.)*	The non-active Real-Time Server Startup is complete when the following message appears in the Event Display: 'Successfully performed Name Server register on RMS pt-to-pt endpoint'	
62.	**The Real-Time Server Hardware Failover test follows.**	Only information, no result or output, is expected.	
63.	**EOC User Station 1**: Create a backup logical string on Real-Time Server 1 by entering the following in the ECL directive line of the Control Window: ECL> **STRING CREATE BACKUP SERVER=1 STRING=100** *(Wait for the completion of the backup directive before going to the next step.)*	The backup string is created, and the following message appears on the Event Display: 'Successfully created backup processing for string 100'	
64.	**EOC User Station 1**: Print the Failover-Monitoring page by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 6' column	
65.	**EOC User Station 1**: Display the number of endpoints for the **active Real-Time Server** by entering the following in a cmdtool window. %: **show.sh** Note the number of endpoints.	There are 33 endpoints on the active Real-Time Server: '(33 rows affected)'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

66.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages are generated for those Ground Script commands executed prior to the WAIT command, indicating successful execution.	
67.	**Real-Time Server 2**: Induce a hardware failure on the active Real-Time Server by pulling the two plugs on the active Real-Time Server connected to the FDDI Concentrator (for DEC) or Ethernet Switch (for SUN) on the Operational LAN. *(Do this in the presence of the FOT System Administrator or representative.)*	The following Event message indicates that the active Real-Time Server has failed: 'Realtime server <number>, host name <server name> failed' The Telemetry Decom page continues updating.	
68.	**EOC User Station 1**: Initiate the failover from the active Real-Time Server to the backup Real-Time Server by entering the following in the ECL directive line of the Control Window: ECL> **STRING FAILOVER STRING=100** *(Wait 60 seconds before executing the next step.)*	Within 60 seconds, the following events will occur: Real-Time Server 2 **temporarily** becomes the **inactive** server until failover is complete. Event messages appear indicating that Real-Time Server 1 is coming up as the **active server**. Note: If failover is unsuccessful (i.e., backup and inactive servers are not both 0), an event message will appear notifying the user to delete String 100. The user would do this and then create String 100.	
69.	**EOC User Station 1**: Print the Failover-Monitoring page by entering the following in a cmdtool window: %: **snapframe**	The Failover-Monitoring page, which appears on the printer, contains the values shown in Table SYS-2030B-1, under the 'Snap 7' column.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

70.	**EOC User Station 1**: Display the number of endpoints for the **active server** by entering the following in a cmdtool window: %: **show.sh** Note the number of endpoints.	The number of endpoints is the same as it was before the failure. The Telemetry Decom page continues updating. Event messages are generated as expected.	
71.	**EOC User Station 1**: Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. Event messages confirm command execution. The user has access to data (files) and the data base.	
72.	**Real-Time Server 2**: Re-insert the plug on Real-Time Server 2. *(Re-insert the plug in the presence of the FOT System Administrator or representative.)*	Real-Time Server 2 is ready for startup. The following event message appears: 'Realtime server <server number>, host name <server name>, available'	
73.	**The Data Server Software Failover test follows.**	Only information, no result or output, is expected.	
74.	**EOC User Station 1**: Display the number of endpoints for the **Data Server** by entering the following in a cmdtool window: %: **show.sh** Note the number of endpoints.	Two sets of endpoints are displayed.	
75.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages indicating successful execution are generated for those Ground Script commands executed prior to the WAIT command.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

76.	**EOC User Station 1**: Simulate a software failure by gracefully terminating all processes on the **Data Server**. Enter the following in a cmdtool window associated with the Data Server: %: **MyKill** *(Wait until all processes terminate.)* Enter the following in a cmdtool window: %: **rm.sh** Note the number of endpoints.	The Telemetry Decom page continues updating. The number of endpoints for the Data Server is zero.	
77.	**EOC User Station 1**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the **non-active** Data Server (i.e., the server that did not just fail). *(Wait for the completion of Data Server startup.)*	Data Server initialization is complete.	
78.	**EOC User Station 1**: Display the number of endpoints for the **new active server** by entering the following in a cmdtool window: %: **show.sh** Note the number of endpoints.	The number of endpoints is the same as it was before the failure. The Telemetry Decom page continues updating. Event messages are generated as expected.	
79.	**EOC User Station 1**: Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. Event messages confirm command execution. The user has access to data (files) and the data base.	
80.	**The Data Server Hardware Failover test follows.**	Only information, no result or output, is expected.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

81.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages indicating successful completion are generated for those Ground Script commands executed prior to the WAIT command.	
82.	**Data Server**: Induce a Data Server failure by pulling the two plugs on the Data Server connected to the FDDI Concentrator (for DEC) or Ethernet switch (for SUN) on the Operational LAN. *(Do this in the presence of the FOT System Administrator or representative.)*	Within 3 minutes, an event message indicates that the Data Server has failed. The Telemetry Decom page continues updating.	
83.	**EOC User Station 1**: Enter the following in the same cmdtool window associated with the unplugged Data Server: %: **rm.sh** Note the number of endpoints.	The Telemetry Decom page continues updating. The number of endpoints for the Data Server is zero.	
84.	**EOC User Station 1**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the **non-active** Data Server (i.e., the server that did not just fail). *(Wait for the completion of Data Server startup.)*	Data Server initialization is complete. Data Server startup completes within 5 minutes.	
85.	**EOC User Station 1**: Display the number of endpoints for the **new active server** by entering the following in a cmdtool window: %: **show.sh** Note the number of endpoints.	The number of endpoints is the same as it was before the failure. The Telemetry Decom page continues updating. Data Server event messages are generated as expected.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

86.	Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. Event messages confirm successful Ground Scripts execution. The user has access to data (files) and the data base.	
87.	**Data Server**: Re-insert the plug on the failed Data Server. *(Re-insert the plug in the presence of the FOT System Administrator or representative.)*	The failed Data Server is ready for future use.	
88.	**EOC User Station 1**: Terminate all processes on the **Data Server (the server on which the plug was pulled**) by entering the following in a cmdtool window: %: **MyKill** *(Wait until the UNIX prompt is received.)* %: **rm.sh**	The number of endpoints for the initial Data Server is zero.	
89.	**The File Server Failover test follows.**	Only information, no result or output, is expected.	
90.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages indicating successful completion are generated for those Ground Script commands executed prior to the WAIT command.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

91.	**File Server**: Induce a File Server failure by pulling the two plugs on the File Server connected to the FDDI Concentrator on the Operational LAN. *(Do this in the presence of the FOT System Administrator or representative.)*	Within 3 minutes, an event message indicates that a File Server has failed. The Telemetry Decom page continues updating.	
92.	**EOC User Station 1**: Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. A new Ground Script can be successfully executed. Event messages confirm successful Ground Scripts execution. The user has access to data (files) and the data base.	
93.	**EOC User Station 1 & File Server**: Write out any pending information from the File Server to the disks, and then stop the processor by entering the following in a cmdtool window: %: **halt** Re-insert the plug on the failed File Server. Reboot the failed File Server. *(Re-insert the plug and reboot in the presence of the FOT System Administrator or representative.)*	The failed File Server is successfully rebooted and ready for future use.	
94.	**The Network (Router) Failover test follows.**	Only information, no result or output, is expected.	
95.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages indicating successful execution are generated for those Ground Script commands executed prior to the WAIT command.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

96.	**Primary EOC Router**: Induce a Network (Router) failure by powering off the Primary EOC Router. *(Do this in the presence of the FOT System Administrator or representative.)*	The event message indicates a failure of the Primary EOC Router. The Telemetry Decom page continues updating.	
97.	**Real-Time Server** **Data Server** **File Servers** **EOC user stations**: Run the scripts to switch to the Secondary EOC Router on the following equipment: Real-Time Server Data Server File Servers EOC user stations Once each switch script is complete, reboot the equipment.	The Secondary EOC Router is active, and the equipment is successfully rebooted. Note: If necessary, run the Startup Scripts for the Real-Time Server, Data Server, and EOC user stations.	
98.	**EOC User Station 1**: Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. A new Ground Script can be successfully executed. Event messages confirm successful Ground Scripts execution. The user has access to data (files) and the data base.	
99.	**Primary EOC Router**: Power up the Primary EOC Router. *(Power-up in the presence of the FOT System Administrator or representative.)*	The Primary EOC Router is powered up.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

100.	**Real-Time Server** **Data Server** **File Servers** **EOC user stations:** Run the scripts to switch back to the Primary EOC Router on the following equipment: Active Real-Time Server Active Data Server Both File Servers EOC user stations Once each switch script is complete, reboot the equipment.	The Primary EOC Router is active, and the equipment is successfully rebooted. Note: If necessary, run the Startup Scripts for the Real-Time Server, Data Server, and EOC user stations.	
101.	**The Network (LAN) Failover test follows.**	Only information, no result or output, is expected.	
102.	**EOC User Station 1**: Execute a Ground Script by entering the following in the CMD field of the 'Command Control Window': **START E2ATC16DG** *(Go to the next step during a WAIT command, while there are still unexecuted commands remaining in the Ground Script.)*	Event messages indicating successful completion are generated for those Ground Script commands executed prior to the WAIT command.	
103.	**Operational LAN**: Induce a Network (LAN) failure by powering down the FDDI Concentrators and Ethernet switches connected to the servers and user stations on the Operational LAN. *(Power-down in the presence of the FOT System Administrator or representative.)*	The event message indicates a failure of the Operational LAN. The Telemetry Decom page continues updating.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

104.	**EOC User Stations 1 & 2**: Terminate all processes and endpoints on the **following equipment** *(Wait until the UNIX prompt is received.)*: Real-Time Server Data Server EOC user stations by entering the following in a cmdtool window. %: **MyKill** **%**:**rm.sh**	The number of endpoints for all equipment is zero.	
105.	**Real-Time Server** **Data Server** **File Servers** **EOC user stations**: Run the scripts to switch to the Support LAN on the following equipment: Real-Time Server Data Server Both File Servers EOC user stations Once each switch script is complete, reboot the equipment.	The Support LAN is active, and the equipment is successfully rebooted.	
106.	**EOC User Station 1**: Execute applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the Data Server, User Station, and Real-Time Server. *(Wait for the completion of Data Server, User Station, and Real-Time Server startup.)*	Data Server initialization is complete. User station startup is complete when the Control Window appears on the EOC user station. Real-Time Server startup is complete when the following message appears in the Event Display: 'String 100 was created.'	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

107.	**EOC User Station 1**: Execute 'Post-Failure Check-out Subprocedure.'	The remainder of the partially executed Ground Script can be completed successfully. A new Ground Script can be successfully executed. Event messages confirm successful Ground Scripts execution. The user has access to data (files) and the data base.	
108.	**Operational LAN**: Power up the FDDI Concentrators and Ethernet switches connected to the servers and user stations on the Operational LAN. *(Power-up in the presence of the FOT System Administrator or representative.)*	The Operational LAN is powered up.	
109.	**EOC User Station 1**: Terminate all processes on the following equipment *(Wait until UNIX prompt is received.)*: Active Real-Time Server Active Data Server EOC user stations by entering the following in a cmdtool window: %: **MyKill** %: **show.sh**	The number of endpoints for all equipment is zero.	

Table B-1. Failure Recovery and Status Monitoring Test Procedure (continued)

110.	**Real-Time Server** **Data Server** **File Servers** **EOC user stations**: Run the scripts to switch back to the Operational LAN on the following equipment: Active Real-Time Server Active Data Server Both File Servers EOC user stations Once each switch script is complete, reboot the equipment.	The Operational LAN is active, and the equipment is successfully rebooted.	
111.	**EOC User Station 1**: Execute the applicable steps of the 'FOS Server and User Station Startup and Shutdown' (SYS-2000B) procedure to bring up the Data Server, User Station, and Real-Time Server. *(Wait for the completion of Data Server, User Station, and Real-Time Server startup.)*	Data Server initialization is complete. User station startup is complete when the Control Window appears on the EOC user station. Real-Time Server startup is complete when the following message appears in the Event Display: 'String 100 was created.'	
112.	**EOC User Station 1**: Stop the flow of telemetry. Enter the following ECL directive: ECL> **PG STOPDATA APID=2**	The Telemetry Decom page is no longer updated.	
113.	Test End		

Table B-2. SYS-2030B-1 Failure Recovery and Status Monitoring Parametric Mnemonic Values

Parameter Mnemonic	Snap 1	Snap 2	Snap 3	Snap 4	Snap 5	Snap 6	Snap 7
System Parameters							
SYS_ACTIVE_STRING_ID							
SYS_STRING_ID	100	100	100	100	100	100	100
SYS_DATA_SRC	Realtime	Realtime	Realtime	Realtime	Realtime	Realtime	Realtime
SYS_DATA_TYPE	1	1	1	1	1	1	1
SYS_SC_ID	AM1	AM1	AM1	AM1	AM1	AM1	AM1
SYS_MODE	OPS	OPS	OPS	OPS	OPS	OPS	OPS
SYS_DB_ID	1.0	1.0	1.0	1.0	1.0	1.0	1.0
SYS_CMD_AUTHOR_ID	<EOC user 1>	<EOC user 2>	<EOC user 1>	<EOC user 1>	<EOC user 1>	<EOC user 1>	<EOC user 1>
SYS_CMD_AUTHOR_WS_ID	<EOC user station 1>	<EOC user station 2>	<EOC user station 1>	<EOC user station 1>	<EOC user station 1>	<EOC user station 1>	<EOC user station 1>
SYS_GRND_CNTRL_ID	<EOC user 1>	<EOC user 2>	<EOC user 2>	<EOC user 1>	<EOC user 1>	<EOC user 1>	<EOC user 1>
SYS_GRND_CNTRL_WS_ID	<EOC user station 1>	<EOC user station 2>	<EOC user station 2>	<EOC user station 1>	<EOC user station 1>	<EOC user station 1>	<EOC user station 1>
SYS_RTS_ID	1	1	1	1	2	2	1
SYS_BACKUP_RTS_ID	0	0	0	2	0	1	0
SYS_INACTIVE_RTS_ID	0	0	0	0	1, then 0	0	2, then 0
SYS_STATE	Active	Active	Active	Active	Active	Active	Active
SYS_USER_ID							
SYS_WKS_ID							

Abbreviations and Acronyms

A_o	Operational Availability
AT	Acceptance Test
CCB	Configuration Control Board
CDRL	Contract Data Requirements List
CM	Configuration Management
COTS	Commercial Off-the-Shelf
CSMS	Communications and Systems Management Segment
DAACs	Distributed Active Archive Centers
DCN	Document Change Notice
DID	Data Item Description
DM	Data Management
ECL	ECS Command Language
ECS	EOSDIS Core System
EDF	ECS Development Facility
EOC	EOS Operations Center
EOS	Earth Observing System
EOSDIS	Earth Observing System (EOS) Data and Information System (DIS)
ESN	EOSDIS Science Network
FDDI	Fiber-optic Distributed Data Interface
FOS	Flight Operations Segment
GSFC	Goddard Space Flight Center
HW	Hardware
IMS	Information Management System
IST	Instrument Support Terminal
LMC	Local Maintenance Coordinator
LRU	Line Replaceable Unit

M&O	Maintenance and Operations
MD	Maintainability Demonstration
MDT	Mean Down Time
MSS	Management Subsystem
MTTR	Mean Time To Repair
NA	Network Administrator
NASA	National Aeronautics and Space Administration
OEM	Original Equipment Manufacturer
PAR	Performance Assurance Requirements
PPM	Principal Period of Maintenance
RAID	Redundant Array of Independent Disks
RMA	Reliability, Maintainability, and Availability
SA	System Administrator
SDPS	Science Data Processing Segment
SEO	Sustaining Engineering Organization
SMC	System Monitoring and Coordination Center
SW	Software
TOO	Target Of Opportunity
UPS	Uninterruptable Power Supply